REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

I. REJECTION OF CLAIMS 1, 12-14 AND 16-18 UNDER 35 U.S.C. § 102

Claims 1, 12-14 and 16-18 stand rejected as being anticipated by the Aura patent (United States Patent No. 6,711,400, issued March 23, 2004, hereinafter "Aura"). The Applicants respectfully traverse the rejection.

Aura teaches an authentication method for telecommunications systems. A mobile station wishing to join a network generates a first random number and sends this first random number in a message that is routed to an associated authentication center. In turn, the authentication center identifies a cipher key for the mobile station, based on the subscriber ID. The authentication center then generates a second random number and enters the cipher key and the first and second random numbers into three one-way hash functions, which provide three additional keys. One of the three additional keys and the second random number are sent to the mobile station, which enters the first and second random numbers, the additional key and the cipher key into the same hash function used by the authentication center. If the mobile station produces the same value for the additional key as that received from the authentication center, the mobile station has successfully identified the network. One of the three additional keys is then accepted as the connection-specific key for communication between the mobile station and the network.

The Examiner's attention is directed to that fact that Aura fails to disclose or suggest the novel method of encrypting a message to be sent including an expected nonce value and a new nonce value, as positively claimed by the Applicants. Specifically, Applicants' independent claims 1, 13, 16 and 18 recite:

> 1. A secure method of transmitting a message between a sender node and a recipient node within a network collaboration group, the sender and

the recipient sharing a secret encryption key and an expected nonce value comprising:

generating a new nonce value known to the sender;

encrypting the message including the expected nonce value and the new nonce value, using the encryption key;

transmitting the encrypted message from the sender to the recipient; and

verifying, by the recipient, that the encrypted message includes the expected nonce value. (Emphasis added)

13. A system for managing communications within a network collaboration group, comprising:

means for generating a new nonce value;

means for incorporating an expected nonce value and the new nonce value in a message to be transmitted;

means for encrypting the message;

means for transmitting the encrypted message from a sender node of the group to a recipient node of the group; and

means for verifying, by the recipient node, that the encrypted message includes the expected nonce value. (Emphasis added)

16. A data-carrying signal for transmitting information securely between a master node and a member node of a network collaboration group, the signal being encrypted using an encryption key shared by the master and the member, the signal comprising:

the information to be transmitted;

an expected nonce value known to the master and the member; and

a new nonce value, different than the expected nonce, provided by a sender of the signal. (Emphasis added)

18. A method for transmitting secure messages between a master node and a member node of a network collaboration group comprising:

encrypting-messages using a key shared by the master and the member, so as to protect confidentiality of the message; and

embedding a plurality of updated nonce values within said encrypted messages so as to provide verifiable integrity, authenticity, and freshness for each of said messages. (Emphasis added)

The Applicants' invention is directed to methods and protocols for intrusion-tolerant management of collaborative network groups. As global users continue their

migration to online network environments, the problem of vulnerability to malicious attacks (*e.g.*, by unauthorized users or "hackers") becomes more severe. Correspondingly, the need for "private" online groups that are resistant to intrusion by unauthorized users increases. Many known methods for providing private, secure communication channels for authorized users (such as virtual private networks or VPNs) remain vulnerable to unauthorized intrusions such as replay attacks (illegitimate interception, copying and re-transmission of legitimate, encrypted traffic). To preserve system integrity and availability, it is important that such attacks be recognized as illegitimate communications.

The Applicants' invention provides a means for transmitting a message from sender to recipient in an intrusion-tolerant manner. Communications between sender and recipient are encrypted with a cryptographic key and include two nonce values in addition to the message. The first nonce value is an expected nonce value, already known to the receiver, while the second nonce value is a new nonce value generated by the sender. When the receiver receives the encrypted message, the receiver verifies that the message includes the expected nonce value. The presence of the expected nonce value confirms that the message is a legitimate message from the sender and is not part of an attack by an unauthorized party. The new nonce value then becomes the expected nonce value for a subsequent message (*e.g.*, from receiver to sender).

By contrast, Aura only teaches a method for authenticating a mobile station, and does not teach the transmission of an encrypted message that includes a plurality of nonce values (*e.g.*, a first nonce value and a second nonce value). At most, Aura merely teaches a hash-based authentication protocol that uses two random numbers (RAND1 and RAND2) and a shared key (K_i).

In particular, Aura does not teach, anywhere, that the information or messages exchanged between the mobile station and the authentication center are encrypted. In fact, the method taught by Aura requires that these messages be transmitted "in the clear" (*e.g.*, unencrypted). For instance, the verification performed by Aura (*e.g.*, as depicted in Fig. 4 of Aura at reference numeral 407) merely teaches the use of one-way hash functions. As explained by Aura, it is very difficult to calculate the contents of a

hashed message (*e.g.*, one cannot determine the key K from knowledge of H(K, X1, X2), even if one knows the values of the argument pairs X1 and X2) (*See*, Aura, Column 6, lines 48-65). Hence, Aura's method cannot be used to transmit an encrypted or previously unknown message from sender to recipient; Aura requires the value RAND2 (which is unknown to the mobile station) to be sent "in the clear", as depicted in Fig. 4 of Aura at reference numeral 406, to enable the checking of the hashed message SRES1. This stands in contrast to the Applicants' use of encryption, where the message transmitted from sender to recipient is $Encrypt_K$(Message, Expected-Nonce, New-Nonce). Under an encryption scheme such as that claimed by the Applicants, where both parties know the key, K, the recipient can decrypt the message to learn the value of both the Message and the New-Nonce.

Thus, Aura fails to teach or suggest a method in which at least two nonce values are transmitted in an encrypted message, as claimed in Applicants' independent claims 1, 13, 16 and 18. Therefore, the Applicants submit that independent claims 1, 13, 16 and 18 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claims 12, 14 and 17 depend from claims 1, 13 and 16 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 12, 14 and 17 are not anticipated by the teachings of Aura. Therefore, the Applicants submit that dependent claims 12, 14 and 17 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

II. REJECTION OF CLAIMS 2-11 AND 15 UNDER 35 U.S.C. § 103

Claims 2-11 and 15 stand rejected as being made obvious by Aura in view of the Janson et al. patent (United States Patent No. 5,729,608, issued March 17, 1998, hereinafter "Janson"). The Applicants respectfully traverse the rejection.

Aura has been discussed above. Janson teaches a method and system for providing secure key distribution in a communication system. In one embodiment, a two-party authentication protocol between user A and user B who share a key, K_{ab}, involves user A transmitting its identity, A, and a nonce, N_{ab}, to user B. User B then generates a new nonce, N_{ba}, and computes the value of an authentication function

AUTH(K_{ab}, N_{ab}, N_{ba}, B), where the value of the authentication function is dependent upon user B's identity, B, the newly generated nonce, N_{ba}, the key, K_{ab}, and the nonce received from A, N_{ab}. User B then transmits the computed value of the authentication function and the newly generated nonce, N_{ba}, to user A, who recomputes the value of the authentication function. If the value recomputed by user A matches the value transmitted by user B, user A authenticates user B. User B then authenticates user A in a similar manner based upon a second authentication function first computed by user A.

The Examiner's attention is directed to the fact that Janson, like Aura fails to disclose or suggest the novel method of providing both an expected nonce value and a new nonce value in an encrypted message, as positively claimed by the Applicants. Applicants' independent claims 1 and 13 have been recited above. In fact, the portions of Janson that the Examiner cites to support the rejection (*i.e.*, step 202 of Fig. 2) teach no more than the use of hash functions. Janson's method, like Aura's, cannot be used to transmit an encrypted or previously unknown message from sender to recipient; Janson requires the computed authentication function value AUTH(K_{ab}, N_{ab}, N_{ba}, B) and the newly generated nonce, N_{ba}, (which is unknown to the user A) to be sent in the clear, to enable the checking of the authentication function value AUTH(K_{ab}, N_{ab}, N_{ba}, B) by user A. Thus, Janson does not provide any relevant additional teachings with regard to Aura.

As discussed above, Aura fails to teach or suggest a method in which at least two nonce values are transmitted in an encrypted message, as claimed in Applicants' independent claims 1 and 13. Janson fails to bridge this gap in the teachings of Aura. Therefore, the Applicants respectfully submit that independent claims 1 and 13, fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-11 and 15 depend, respectively, from claims 1 and 13 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2-11 and 15 are not made obvious by the teachings of Aura in view of Janson. Therefore, the Applicants submit that dependent claims 2-11 and 15 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

III. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

10/27/05
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702